

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

SURFSIDE NON-SURGICAL)	
ORTHOPEDICS P.A., individually and on)	
behalf of all others similarly situated,)	
)	
Plaintiff,)	
)	No. 18 C 566
v.)	
)	Judge Sara L. Ellis
ALLSCRIPTS HEALTHCARE SOLUTIONS,)	
INC.,)	
)	
Defendant.)	

OPINION AND ORDER

In January 2018, malware infected servers belonging to Allscripts Health Care Solutions, LLC (“LLC”), a healthcare information technology (“IT”) company. The attack temporarily disrupted service to customers, including Plaintiff Surfside Non-Surgical Orthopedics (“Surfside”). Surfside consequently brought a putative class action against Defendant Allscripts Healthcare Solutions, Inc. (“INC”), the parent company to LLC, alleging negligence, breach of contract, unjust enrichment, as well as violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/2, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a)(5), (7). INC moves to dismiss Surfside’s claims on the grounds that Surfside lacks standing to sue and has failed to adequately plead its claims. Because Surfside has not shown that INC caused the injury of which it complains, the Court dismisses the complaint for lack of standing.

BACKGROUND¹

I. Allscripts' Corporate Structure

INC is a holding company of several subsidiaries that provide IT products and services to healthcare organizations. INC is incorporated in Delaware with its principal place of business in Chicago, Illinois. As a non-operating entity, it has no paid employees and does not sell any products or provide any services. It has eight officers whose responsibilities include interfacing with the investment community and preparing public filings with the Securities and Exchange Commission ("SEC"). All eight of the officers are employed by LLC and perform work on behalf of INC using LLC computers and equipment.

LLC, based out of Raleigh, North Carolina, is an indirect subsidiary three levels below INC in a complex corporate structure. It provides healthcare solutions, i.e. proprietary software related to electronic health records ("EHR"), as well as hosting services to thousands of physicians, hospitals, and other healthcare providers. Its hosting environment includes data centers located in North Carolina in a separate location from the corporate office.

II. LLC's Contract with Surfside and the 2018 Malware Attack

Surfside, a medical practice located in Boynton Beach, Florida, purchased subscriptions from LLC for EHR solutions and hosting services in 2014, and again in 2017. The subscription also included technical services related to "meaningful use" attestation—verification that Surfside's EHR met certain government standards that allowed it to qualify for Medicare and Medicaid reimbursements.

¹ The facts in the background section are taken from the complaint and additional materials submitted by the parties to determine the motion to dismiss for lack of subject matter jurisdiction. *Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 444 (7th Cir. 2009).

In January 2018, a strain of ransomware called “SamSam” infected 2,100 of LLC’s servers in North Carolina. Ransomware is a type of malware that encrypts data on the victim’s computer and demands payment in exchange for unlocking it. The attack temporarily prevented Surfside from accessing EHR and e-prescribing medication to patients.

III. Deposition of Edward Dillon

Following the ransomware attack, Surfside filed this class action against INC. At the request of the parties, the Court ordered limited jurisdictional discovery. As part of this process, Surfside deposed Edward Dillon, the assistant treasurer of INC and vice president and corporate controller for LLC. Pertinent to this Opinion, Dillon explained that LLC was directly involved in and responsible for responding to the ransomware attack. LLC leadership and management teams set the budget for cybersecurity activities, drafted the IT security and privacy policies, and were responsible for implementing these policies. LLC also owned and operated the data centers containing the servers affected by the attack.

INC, on the other hand, was not involved in the cybersecurity response to the ransomware attack. Its purpose as a holding company is to present a publicly-traded corporation with many subsidiaries as a single entity to outside investors. As such, INC’s concern was with the impact on the investment community. At the time of the attack INC was preparing the 10-k form, which INC files annually with the SEC to provide information to investors. The 10-k describes security breaches as a risk to the company, including the attack in this case: “Recently, we were subject to a ransomware attack that impacted two of our data centers, resulting in outages that left certain of our solutions offline for our clients.” Doc. 87, Ex. A (“10-k”) at 25.² The 10-k also states that because INC deals with protected health information, it is subject to

² Where the ECF header differs from the page number of the original document, as it does here, this Opinion cites to the original document.

requirements under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”): “HIPAA applies to ‘Covered Entities,’ such as certain healthcare providers, health plans, and healthcare clearinghouses We consider ourselves a Covered Entity due to our acting as a ‘healthcare clearinghouse.’” *Id.* at 8. It further states: “In addition . . . we are, in some circumstances, considered a business associate under HIPAA. As a business associate, we are subject to the HIPAA requirements relating to the privacy and security of protected health information.” *Id.* While the 10-k does not differentiate between INC and LLC, it states that “[e]ach of the terms ‘we,’ ‘us,’ ‘our’ or ‘company’ as used herein refers collectively to Allscripts Healthcare Solutions, Inc. and its wholly-owned subsidiaries and controlled affiliates, unless otherwise stated.” *Id.* at 3, 73.

Dillon also testified regarding thirteen e-mails sent to clients affected by the ransomware attack. The bottom of each e-mail included language stating: “This email was sent by: Allscripts Healthcare Solutions, Inc 222 Merchandise Mart Plaza, 20th Floor Chicago, IL 60654 USA.” Doc. 92, Ex. B (“Dillon Dep.”) at 70:17–78:8, Ex. B6–B13. An LLC employee drafted these emails and sent them through a third-party tool kit to LLC clients. According to Dillon, INC did not have the capacity to send these e-mails because they are non-operational. Dillon Dep. 83:8–12. When counsel for Surfside asked why the e-mails stated they were sent by INC, Dillon responded that “it happened to be the template that was utilized when [the employee] prepared it for his LLC client base.” *Id.* at 82:10–12.

Finally, Dillon testified that INC carries an insurance policy that covers all its subsidiaries. While INC is the insured party, interactions with the insurance carrier occur through LLC, not through INC.

IV. Affidavit of Glen Chapman

Surfside's CEO, Glenn Chapman, produced an affidavit stating that Surfside was required to submit documentation to the Centers for Medicare and Medicaid Services ("CMS") attesting that its EHR programs met meaningful use standards. Mr. Chapman further stated that: "I have contacted Defendant in connection with Surfside's annual CMS submissions, and each year since 2014, I have been told by Defendant to submit the same 'Allscripts Security Overview' document to CMS." Doc 87, Ex. K at 1. The security overview states that it is "the confidential property of," and copyrighted by, INC. Doc. 87, Ex. L at 2.

V. Security Policies

The parties submitted 2015 and 2017 editions of the "Allscripts HIPAA Privacy Policy." Doc. 87, Ex. J; Doc. 100. The 2015 edition is silent on whether it is an INC or LLC policy. The 2017 edition notes that it is the copyright and property of LLC. Both policies list the Privacy and Security Executive Council ("PSEC")—a group of LLC managers—as the approval authority.

The parties also submitted 2016 and 2018 editions of the "Information Security Management Policy" ("security policy"). The 2016 version states that the "methodology and models presented herein are proprietary with copyrights, Allscripts Healthcare Solutions, Inc." Doc. 92 Ex. B14 at 1. The 2018 version states that it is "proprietary with copyrights of Allscripts Healthcare, LLC." Doc. 99 at 1. Both policies list the approval authority as the PSEC.

LEGAL STANDARD

A motion to dismiss under Rule 12(b)(1) challenges the Court's subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1). The party asserting jurisdiction has the burden of proof. *United Phosphorus, Ltd. v. Angus Chem. Co.*, 322 F.3d 942, 946 (7th Cir. 2003), *overruled on other grounds by Minn-Chem, Inc. v. Agrium, Inc.*, 683 F.3d 845 (7th Cir. 2012). The standard

of review for a Rule 12(b)(1) motion to dismiss depends on the purpose of the motion. *Apex Digital, Inc. v. Sears, Roebuck & Co.*, 572 F.3d 440, 443–44 (7th Cir. 2009). If a defendant challenges the sufficiency of the allegations regarding subject matter jurisdiction (a facial challenge), the Court must accept all well-pleaded factual allegations as true and draw all reasonable inferences in the plaintiff’s favor. *See id.*; *United Phosphorus*, 322 F.3d at 946. If, however, the defendant denies or controverts the truth of the jurisdictional allegations (a factual challenge), the Court may look beyond the pleadings and view any competent proof submitted by the parties to determine if the plaintiff has established jurisdiction by a preponderance of the evidence. *See Apex Digital*, 572 F.3d at 443–44; *Meridian Sec. Ins. Co. v. Sadowski*, 441 F.3d 536, 543 (7th Cir. 2006).

ANALYSIS

“[N]o principle is more fundamental to the judiciary’s proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.” *Spokeo, Inc. v. Robins*, --- U.S. ---, 136 S. Ct. 1540, 1547, 194 L. Ed. 2d 635 (2016) (quoting *Raines v. Byrd*, 521 U.S. 811, 818, 117 S. Ct. 2312, 138 L. Ed. 2d 849 (1997)). Standing is a central requirement of this principle. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992). The “constitutional minimum” of standing has three basic components: (1) the plaintiff must have suffered an injury-in-fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision. *Id.* at 560–61. INC argues that Surfside cannot demonstrate the last two components because INC is a non-operating holding company with no relationship to Surfside, and it bears no responsibility for the ransomware attack. In response, Surfside contends that INC is a holding company in name only, and that its direct involvement in

cybersecurity activities means Surfside can hold it liable as a direct participant in the wrongdoing. *Forsythe v. Clark USA, Inc.*, 864 N.E.2d 227, 241, 309 Ill. Dec. 361 (Ill. 2007).

The Court first addresses the causation prong, which is the main focus of the parties' briefs.

I. Causation

"It is a general principle of corporate law deeply 'ingrained in our economic and legal systems' that a parent corporation (so-called because of control through ownership of another corporation's stock) is not liable for the acts of its subsidiaries." *United States v. Bestfoods*, 524 U.S. 51, 61, 118 S. Ct. 1876, 141 L. Ed. 2d 43 (1998) (quoting William O. Douglas & Carol M. Shanks, *Insulation from Liability Through Subsidiary Corporations*, 39 Yale L.J. 193 (1929)). However, liability still attaches in "instances where the parent is directly a participant in the wrong complained of." *Forsythe*, 864 N.E.2d at 233 (quoting Douglas & Shanks, *supra*, at 208). This usually arises when the parent interferes with or overrides the internal operations of the subsidiary and "the alleged wrong can seemingly be traced to the parent through the conduit of its own personnel and management." *Bestfoods*, 524 U.S. at 64 (quoting Douglas & Shanks, *supra*, at 207). The direct participant theory of liability "does not rest on piercing the corporate veil." *Forsythe*, 864 N.E.2d at 241.³ Instead, liability is based on "a parent's direct participation, superseding the discretion and interest of the subsidiary, and creating conditions leading to the activity complained of." *Id.*

Surfside consistently describes INC as being "directly responsible," playing a "direct role," and having "direct responsibility" for the failed security that led to the ransomware attack. Doc. 87 at 3, 7, 9. It first points to Dillon's deposition to argue that "[t]he key people required to be notified of a cybersecurity attack are the officers and directors of INC," specifically the CEO,

³ Recognizing this, Surfside does not attempt to pierce the corporate veil in order to place liability on INC. Doc. 51 ¶ 6.

CFO, chief delivery officer, general counsel, and the secretary. Doc. 87 at 7–8. This is not an accurate characterization of Dillon’s testimony. Dillon stated that these INC executives also held senior management positions within LLC, and they consequently learned about the ransomware attack on a real-time basis in their capacity as LLC employees. Dillon Dep. 42:17–46:1. In their INC capacities, these officers were concerned about the incident because of its impact on the investment community. *Id.* at 47:20–48:11. Dillon stated repeatedly that LLC, not INC, had responsibility for responding to the ransomware attack. *Id.* at 47:5–6, 55:23–24, 63:23–64:9, 83:5–12, 85:20–21, 86:19–21, 97:13–14, 100:3–7, 102:1–6. To argue the senior management’s overlapping roles proves INC was involved in the company’s cybersecurity activities ignores the “well established principle [of corporate law] that directors and officers holding positions with a parent and its subsidiary can and do ‘change hats’ to represent the two corporations separately, despite their common ownership.” *Bestfoods*, 524 U.S. at 69 (quoting *Lusk v. Foxmeyer Health Corp.*, 129 F.3d 773, 779 (5th Cir. 1997)).

Surfside also argues that the 10-k form shows INC’s involvement because it states: “[w]e consider *ourselves* a Covered Entity,” “*we* were subject to a ransomware attack that impacted two of *our* data centers,” and “*we* maintain insurance coverage . . . designed to address certain aspects of security-related risks.” 10-k at 8, 25 (emphasis added). Surfside ignores that the 10-k explicitly states that language such as “we” and “our” refers to INC and its subsidiaries. *Id.* at 3, 73. Courts have also found that inclusive references in public filings are common practice. *E.g.*, *Corp. Safe Specialists, Inc. v. Tidel Techs., Inc.*, No. 05 C 3421, 2005 WL 1705826, at *5 (N.D. Ill. July 15, 2005) (“The Internal Revenue Service, SEC, and generally accepted accounting principles, all allow parent companies to consolidate their financial activities with that of subsidiary companies in their annual reports.”); *Roberts v. Wells Fargo Bank, N.A.*, No. 4:12-cv-

200, 2013 WL 1233268, at *7 (S.D. Ga. Mar. 27, 2013) (noting that a holding company is “a corporation designed only to own other corporations and profit from that ownership” and “isolated references to ‘we’ and ‘ours’ in public disclosures simply do not rebut that”); *Berry v. Bryant*, No. 11-514 JCH-GBW, 2012 WL 12819204, at *5 (D.N.M. Mar. 15, 2012) (“[R]eferences by a parent corporation to the business of its subsidiary as being part of the business of the parent does not serve to erase the substantive and legal distinction between corporations.”). Similarly, it is not unusual that INC carries an insurance policy covering all its subsidiaries. *See Watters v. Kirk*, No. 0:12-cv-338-CMC, 2012 WL 831452, at *3 (D.S.C. Mar. 12, 2012) (describing out-of-state parent corporation’s “administrative role in procuring insurance for its subsidiary” as a “normal attribute[] of a parent-subsidiary relationship” and therefore insufficient to establish personal jurisdiction).

Surfside finally points to language on e-mails, the security overview, and the 2016 security policy that states the documents were the property and copyright of INC. The evidence suggests this was likely due to LLC’s carelessness, rather than INC’s active role in IT security. To begin, Dillon testified that an LLC employee generated the e-mails and sent them to LLC clients through a third-party tool kit. When asked why they state copyright of INC, he responded that it “happened to be the template that was utilized when [the employee] prepared [the e-mails].” Dillon Dep. at 82:10–12. He further stated that he did not know why this template was used and repeated several times that INC did not have the operational capacity to send the e-mails. It is unclear why INC does not have the capacity to do this because INC officers perform other tasks, such as public filings. And if INC officers do not send e-mails, it would be odd that there was an INC template existed. To find, however, that these e-mails demonstrate INC’s direct involvement in security protocols, the Court would have to disregard the entirety of

Dillon's deposition testimony. Moreover, because the attack impacted service to LLC clients—and Surfside concedes that INC was not a party to its contract with LLC—it makes sense that an LLC employee generated and sent these e-mails. As such, Surfside asks the Court to draw inferences about INC's involvement that are inconsistent with the majority of the evidence and the Court declines to do so.

Nor does INC's name on the security overview—the document attesting that INC's EHR complied with meaningful use standards—realistically suggest that INC implemented the underlying policies. Although INC does not explain why its name is on the document, the evidence shows that LLC owns and sells the underlying products. Moreover, Surfside purchased technical services related to meaningful use attestation from LLC. With respect to Mr. Chapman's affidavit, it does not describe who instructed him to submit the security overview to the CMS. Because all INC officers are also LLC employees, and because INC is non-operational, the person Mr. Chapman identifies as "the Defendant" was likely acting in the capacity of an LLC employee. Doc. 87, Ex. K at 1.

As INC points out, the security overview is not the security policy itself, which is the more relevant document. The security policies, as well as the HIPAA privacy policies, all state that the PSEC had ultimate approval authority. This was a group of LLC employees. The only portion of the security policies that Surfside link to INC is INC language on the 2016 security policy, which was not in effect at the time of the attack. This was likely another mistake on the part of LLC because the 2018 version was modified to clarify that it was the property and copyright of LLC. *See Corp. Safe*, 2005 WL 1705826, at *5 (finding statements in 10-k, affidavit, and e-mails, attributing subsidiary's activities to parent company, "were no more than

an attorney's mistake" and insufficient to establish parent company acted as alter ego of subsidiary).

In sum, while LLC may have carelessly used INC's name in some documents, that is not a sufficient basis to allow the Court to find that INC qualifies as a direct participant in the incident. *Id.* The majority of the evidence shows that INC's behavior was consistent with normal parent-subsidary behavior. *See, e.g., Bestfoods*, 524 U.S. 51, 69 (officers with overlapping roles are presumed to "change hats"); *Watters*, 2012 WL 831452, at *3 (procuring insurance for subsidiary); *Corp. Safe*, 2005 WL 1705826, at *5 (consolidated 10-k forms). It further demonstrates that INC was a mere holding company that had no part in the security failure that led to the ransomware attack. As such, Surfside has not shown by a preponderance of the evidence that its injury is fairly traceable to INC, and therefore INC is not the proper defendant in this case. *Apex Digital*, 572 F.3d at 443–44; *see also, McNeal v. J.P. Morgan Chase Bank, N.A.*, No. 16 CV 3115, 2016 WL 6804585, at *2 (N.D. Ill. Nov. 17, 2016) (dismissing plaintiff's tort and state law claims for lack of standing because they were not fairly traceable to holding company); *cf. Degenhart v. AIU Holdings, Inc.*, No. C10-5172RBL, 2010 WL 4852200, at *1 (W.D. Wash. Nov. 26, 2010) (finding plaintiff lacked standing because complaint failed to allege that holding company "participated in the decisions, or in setting policies leading to the decisions, allegedly causing plaintiffs' injury").

II. Redressability

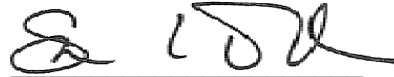
Causation and redressability have been described as "two facets of a single causation requirement." *Allen v. Wright*, 468 U.S. 737, 753 n.19, 104 S. Ct. 3315, 82 L. Ed. 2d 556 (1984), *abrogated on other grounds by Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 S. Ct. 1377, 188 L. Ed. 2d 392 (2014). "[T]he former examines the causal

connection between the assertedly unlawful conduct and the alleged injury, whereas the latter examines the causal connection between the alleged injury and the judicial relief requested.” *Id.* Surfside asks the Court for monetary compensation and “equitable relief compelling Allscripts to utilize appropriate methods and policies with respect to ransomware protection.” Doc. 1 at 22. But if the plaintiff has sued the wrong defendant, the Court cannot redress its injury. *Simon v. E. Kentucky Welfare Rights Org.*, 426 U.S. 26, 41–42, 96 S. Ct. 1917, 48 L. Ed. 2d 450 (1976) (“[T]he ‘case or controversy’ limitation of Art[icle] III still requires that a federal court act only to redress injury that fairly can be traced to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court.”). The evidence shows that INC is non-operational, whereas LLC (1) budgets for cybersecurity activities, (2) drafts the security policies, (3) owns and copyrights the security policies, (4) implements the security policies, (5) owns and operates the servers that were affected by the ransomware attack, and (6) is responsible for responding to security breaches. As such, it would be futile for the Court to order INC to implement appropriate security measures. Nor can the Court order damages from the wrong defendant. *Id.*

CONCLUSION

For the foregoing reasons, the Court grants INC’s motion to dismiss for lack of subject matter jurisdiction [81]. The Court dismisses the case without prejudice. Case terminated.

Dated: June 4, 2019


SARA L. ELLIS
United States District Judge